CISM®

CERTIFIED INFORMATION SECURITY MANAGER®

CISM Review Questions, Answers & Explanations Manual 2006 Supplement

Information Systems Audit and Control Association®

Information Systems Audit and Control Association® (ISACA®)
With more than 50,000 members in more than 140 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal®*, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 44,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,500 professionals since inception.

Disclaimer
ISACA has produced this publication as an educational resource to assist individuals preparing to take the CISM certification exam. It was produced independently from the CISM Certification Board, which has had no input into or responsibility for its content. Copies of past examinations are not released to the public and are not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to these or other ISACA/ITGI publications assuring candidates' passage of the CISM examination.

Disclosure

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Web sites: *www.isaca.org*

ISBN 1-933284-40-4
CISM Review Questions, Answers & Explanations Manual 2006 Supplement
Printed in the United States of America

PREFACE

ISACA is pleased to offer this 100 questions, answers and explanations manual. The purpose of this manual is to provide the CISM candidate with sample questions and testing topics to help prepare and study for the CISM examination.

The material for this manual consists of 100 multiple-choice study questions, answers and explanations, which are arranged in the same proportion as the CISM job practice. These questions, answers and explanations are intended to introduce CISM candidates to the types of questions that appear on the CISM examination. They are not actual questions from the exam. Questions are sorted by CISM content areas, and a sample test of 100 questions is also provided. Sample questions contained in this manual are provided to assist the understanding of the material in the *CISM Review Manual 2006* and to depict the type of question format typically found on the CISM exam.

ISACA has produced this publication as an educational resource to assist individuals preparing to take the CISM certification exam. It was produced independently from the CISM Certification Board, which has had no input into or responsibility for its content. Copies of past examinations are not released to the public and are not made available to ISACA for preparation of this publication. ISACA makes no representations or warranties whatsoever with regard to this or other ISACA/ITGI publications assuring candidates' passage of the CISM examination.

ISACA wishes you success with the CISM examination. Your commitment to pursuing the leading certification for information security managers is exemplary, and for this reason, we welcome your comments and suggestions on the use and coverage of this manual. At the end, you will find a feedback questionnaire. After the examination is over, please take a moment to complete and mail this questionnaire back to ISACA. Your observations will be invaluable as new questions, answers and explanations are prepared.

TABLE OF CONTENTS

INTRODUCTION

OVERVIEW

This manual consists of 100 multiple-choice questions, answers and explanations. These questions are selected and provided in two formats.

Questions Sorted by Content Area
Questions, answers and explanations are provided (sorted) by CISM content areas. This allows the CISM candidate to study material by content area and refer to specific questions to evaluate comprehension of the topics covered within each content area. These questions are representative of CISM questions, although they are not actual test items. They are intended to provide the CISM candidate with an understanding of the type and structure of question that would typically appear on the examination.

Sample Test
The 100 questions are also provided as a sample test. Candidates are urged to use this sample test and the answer sheets provided to simulate an actual examination. Many candidates use this exam as a pre-test to determine their own specific strengths or weaknesses, or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. These sample test questions have been cross-referenced to the questions, answers and explanations by area, so it is convenient to refer to the explanations of the correct answers. This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and with the *CISM Review Questions, Answers & Explanations Manual 2006.*

It should be noted that the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement* has been developed to assist a CISM candidate to study and prepare for the CISM examination. As you use this publication to prepare for the examination, please note that it covers a broad spectrum of information security management issues. Do not assume that reading and working the questions in this manual will fully prepare you for the examination. Since examination questions often relate to practical experiences, a CISM candidate is cautioned to refer to his/her own experiences and to other publications referred to in the *CISM Review Manual 2006*. These additional references are an excellent source of further detailed information and clarification. It is recommended that candidates evaluate the job content areas in which he/she feels weak or requires a further understanding, and study accordingly. Also, please note that this publication has been written using standard American English.

TYPES OF QUESTIONS ON THE CISM EXAM

CISM exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. As previously mentioned, all questions are multiple choice and are designed for one best answer.

The candidate is cautioned to read each question carefully. Many times a CISM examination question will require the candidate to choose the appropriate answer that is **MOST** likely or **BEST**. Or, a candidate may be asked to choose a practice or procedure that would be performed **FIRST** related to the other answers. In every case, the candidate is required to read the question carefully, eliminate known wrong answers and then make the best choice possible. Knowing that these types of questions are asked and how to study to answer them will go a long way toward answering them correctly.

Every CISM question has a stem (question) and four options (answer choices). The candidate is asked to choose the correct or best answer from the options. The stem may be in the form of a question or incomplete statement. In some instances, a scenario or description also may be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Please note that questions requiring the candidate to choose one to several items from a list are not used on the CISM examination and should not be used as a study source.

Another condition a candidate should consider when preparing for the examination is to recognize that information security is a global profession, and individual perceptions and experiences may not reflect the more global position or circumstance. Since the examination and CISM manuals are written for the international information security community, a candidate will be required to be somewhat flexible when reading a condition that may be contrary to a candidate's experience. It should be noted that CISM examination questions are written by experienced information security managers from around the world. Each question on the exam is reviewed by ISACA's CISM Test Enhancement Committee and CISM Certification Board, which consist of international members. This geographical representation ensures that all test questions are understood equally in every country and language.

These review manuals are living documents. As technology advances, these manuals will be updated to reflect such advances. Any suggestions to enhance the materials covered herein, or reference materials, should be directed to:

Mail: **ISACA**
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Attention: Manager—Certification Study Program and Educational Development
Phone: +1.847.253.1545, ext. 484
Fax: +1.847.253.1443
E-mail: *efernandez@isaca.org*

QUESTIONS, ANSWERS AND EXPLANATIONS BY AREA

T1 INFORMATION SECURITY GOVERNANCE

T1-1 The **PRIMARY** motivation for developing an information security strategy is to:

A. establish security metrics and performance monitoring.
B. educate business process owners regarding their duties.
C. ensure that legal and regulatory requirements are met.
D. support the business objectives of the organization.

D The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

T1-2 Senior management commitment and support for information security can **BEST** be enhanced through:

A. publishing a formal security policy signed by the CEO.
B. regular security awareness training for new employees.
C. periodic briefings to the senior management team.
D. senior management sign-off on the information security strategy.

C Obtaining "face time" with senior management is critical to obtaining their support. Although having the CEO sign the security policy and senior management sign-off on the security strategy makes for good visibility and demonstrates good tone at the top, it is a one-time discrete event that may be too quickly forgotten by senior management. Security awareness training for new employees will not have as much effect on senior management commitment.

T1-3 When identifying legal and regulatory issues affecting information security, which of the following would represent the **BEST** approach to developing information security policies?

A. Create separate policy versions for each regulation.
B. Develop policies that meet all mandated requirements.
C. Incorporate policy templates provided by regulators.
D. Use commercially available policy templates.

B It will be much more efficient to craft all of the relevant requirements into the policies than to create separate versions. Using templates provided by regulators or those that are commercially available will not capture all of the requirements mandated by different regulators.

T1-4 Which of the following is generally within the scope of an information security governance steering committee?

A. Interviewing candidates for information security specialist positions
B. Developing content for security awareness programs
C. Prioritizing information security initiatives
D. Approving access to critical financial systems

C Prioritizing information security initiatives is the only appropriate item. The interviewing of specialists should be performed by the information security manager while the developing of program content should be performed by the information security staff. Approving access to critical financial systems is the responsibility of individual system data owners.

T1-5 Which of the following is the **MOST** important factor when designing an information security architecture?

A. Technical platform interfaces
B. Scalability of the network
C. Development methodologies
D. Stakeholder requirements

D The most important factor for information security is that it advances the interests of the business, as defined by stakeholder requirements. Interoperability, scalability and development methodologies are all important but are without merit if a technologically elegant solution is achieved that does not meet the needs of the business.

T1-6 Which of the following characteristics would be the **MOST** important to look for in prospective candidates for the role of chief information security officer (CISO)?

A. Knowledge of information technology platforms, networks and development methodologies
B. Ability to understand and map organizational needs to enabling security technologies
C. Knowledge of existing regulatory environment and project management techniques
D. Ability to manage a diverse group of individuals and resources across an organization

B Only with the ability to understand and map organizational needs to enabling security technologies will information security be properly aligned with the goals of the business. All other choices are secondary in importance.

T1-7 Which of the following are likely to be updated **MOST** frequently?

A. Procedures for hardening database servers
B. Standards for password length and complexity
C. Policies addressing information security governance
D. Standards for document retention and destruction

A Policies and standards should generally be more static and less subject to frequent change. Procedures on the other hand, especially with regard to the hardening of operating systems, will be subject to constant change, since as operating systems change and evolve the procedures for hardening will have to keep pace.

T1-8 Who should be responsible for enforcing access rights to application data?

A. Data owners
B. Business process owners
C. The information security steering committee
D. Security administrators

D As custodians, security administrators are responsible for enforcing access rights to data. Data owners are responsible for approving these access rights. Application developers would not be responsible for enforcement.

T1-9 The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

A. Head of internal audit
B. Chief executive officer (CEO)
C. Chief technology officer (CTO)
D. Legal counsel

B The CISO should ideally report to as high a level within the organization as possible. Among the choices given, the CEO would be the highest official. The head of internal audit and legal counsel would make good secondary choices. Reporting to the CTO could become problematic as the CTO's goals for the infrastructure might at times run counter to the goals of information security.

T1-10 Which of the following would be the **MOST** appropriate task for a chief information security officer (CISO) to perform?

A. Update platform-level security settings.
B. Conduct disaster recovery test exercises.
C. Approve access to critical financial systems.
D. Develop information security strategy paper.

D Developing a strategy paper on information security would be the most appropriate. Approving access would be the job of the data owner. Updating platform-level security and conducting recovery test exercises would be less appropriate as these are essentially administrative tasks.

T1-11 Developing a successful business case for the acquisition of information security software products can **BEST** be assisted by?

A. Projecting the frequency of incidents
B. Quantifying the cost of a control failure
C. Calculating return on investment projections
D. Comparing spending against similar organizations

C Calculating the return on investment will most closely align security with the impact on the business. Frequency and cost of incidents are factors that go into determining the impact on the business, but by themselves they are insufficient. Comparing against similar organizations can be problematic, since similar organizations may have different business goals and appetites for risk.

T1-12 Which of the following would be sufficient in ensuring the proper destruction of sensitive business records?

A. Nonremovable magnetic media should be reformatted.
B. Personal information should be rendered unrecoverable.
C. Spoiled forms should be recycled where practical.
D. Backup media no longer needed should be reused for other applications.

B Increasingly, the protection and proper disposal of personal information has become subject to greater scrutiny by regulators. Reformatting may not be sufficient to totally remove this information from magnetic media. Similarly, reusing backup media may expose previously recorded information to disclosure. Finally, spoiled forms containing customer information should be shredded.

T1-13 When the information security manager is developing a strategic plan for information security, the time horizon for the plan should be:

A. aligned with the IT strategic plan.
B. based on the current rate of technological change.
C. three to five years for both hardware and software.
D. aligned with the global business strategy.

D Any planning for information security should be properly aligned with the needs of the business. Technology should not come before the needs of the business, nor should planning be on some artificial timetable that ignores business needs.

T1-14 Which of the following is the **MOST** important information to include in a strategic plan for information security?

A. Information security staffing requirements
B. Current state and desired future state
C. IT capital investment requirements
D. Information security mission statement

B It is most important to paint a vision for the future and then draw a road map from the starting point to the desired future state. Staffing, capital investment and even mission all stem from this foundation.

T1-15 Sequencing of information security projects should be prioritized on the basis of:

A. time required to implement.
B. impact on the organization.
C. total cost to implement.
D. mix of resources required.

B Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time, cost and resource issues should be subordinate to this objective.

T1-16 Which of the following is the **MOST** important item of information to include in an information security standard?

A. Creation date
B. Author name
C. Initial draft approval date
D. Last review date

D The last review date confirms the currency of the standard, affirming that management has reviewed the standard to assure that nothing in the environment has changed that would necessitate an update to the standard. The name of the author is not that important, as is the creation and draft dates.

T1-17 Which of the following is **MOST** likely to be a concern when distributing information security policies electronically?

A. Broken hyperlinks within the documents
B. Version control problems
C. Failure to distribute updates
D. Content being more difficult to understand

A Broken hyperlinks are a common occurrence in which cross-references within the policies to other information may be lost when files are moved. Version control and failure to distribute are common occurrences with nonelectronic distribution. As for readability, electronic versions offer the added benefits of help buttons and links to examples and other explanatory information.

T1-18 How frequently should information security procedures for O/S patch management generally be reviewed and updated?

A. Annually
B. Whenever standards are updated
C. Monthly
D. After every patch implementation

D Procedures for O/S patch management will be subject to constant change, since as operating systems change and evolve, the procedures for applying patches will have to keep pace. Since standards are not updated as often, aligning changes to procedures to changes to standards would be insufficient. Similarly, monthly and annual changes would be inappropriate.

T1-19 Regulatory requirements relating to information security are **MOST** often directed at which of the following?

A. Offsite media storage
B. O/S patch levels
C. Personal information
D. Application recovery

C Increasingly, the protection and proper disposal of personal information has become subject to greater scrutiny by regulators. Patch levels, media storage and application recovery have not been stressed to the same degree.

T1-20 The **BEST** way for the information security manager to prepare for regulatory reviews is to:

A. assign an information security administrator to act as a regulatory liaison.
B. perform periodic self-assessments using regulatory guidelines and reports.
C. circulate previous regulatory reports to applicable process owners.
D. refer all regulatory inquiries to the legal department.

B Self-assessments will provide the best feedback on readiness and permit identification of items requiring remediation. Directing regulators to a specific person or department or circulating previous reports will not be as effective.

T1-21 A global organization is subject to regulation by multiple governmental jurisdictions, each having differing requirements. The information security manager should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
B. establish baseline standards for all locations and add supplemental standards as required
C. bring all locations into conformity with a generally accepted set of industry best practices.
D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

B It will be more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices will cause certain locations to fail to be in regulatory compliance. On the opposite extreme, forcing all locations to be in compliance will all regulations would place an undue burden on those locations.

T2 RISK MANAGEMENT

T2-1 Which of the following is the **PRIMARY** reason for performing risk management?

A. It allows the organization to eliminate all risk.
B. It is a necessary part of management's due diligence.
C. It satisfies many audit and regulatory requirements.
D. It is helpful in calculating return on investment.

B The key reason for performing risk management is that it is part of management's due diligence. The elimination of all risk is not possible. Satisfying audit and regulatory requirements is of secondary importance, as is calculating return on investment.

T2-2 Which of the following groups would be in the **BEST** position to perform a risk analysis for a business?

A. External regulatory auditors
B. A peer group within a similar business
C. Process owners within the organization
D. An established management consultancy

C Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties would not have that level of detailed knowledge on the inner workings of the business. Management consultants would be expected to have the necessary skills in risk analysis techniques but would still be less effective than a group with intimate knowledge of the business.

T2-3 A successful risk management program should lead to:

A. optimization of risk reduction efforts vs. cost.
B. containment of losses to an annual budgeted amount.
C. identification and removal of all man-made threats.
D. elimination or transference of all organizational risks.

A Successful risk management should lead to a break-even point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, and losses cannot be budgeted in advance with absolute certainty.

T2-4 The results of an organizational risk analysis should **FIRST** be shared with:

A. external auditors.
B. stockholders.
C. senior management.
D. peer organizations.

C Senior management is the primary audience for this information. Much of it is confidential, so disclosure of details to outsiders or stockholders could subject the organization to increased risk. The results are likely to be shared with external auditors but not until agreed to and possibly actioned by senior management.

T2-5 Which of the following risks would **BEST** be assessed using quantitative risk assessment techniques?

A. Customer data stolen by a former employee
B. An electrical power outage lasting 18-24 hours
C. An e-commerce web site defaced by hackers
D. The loss of 75 percent of the software development team

B The effect of the theft of customer data or web site defacement by hackers could lead to a permanent decline in customer confidence, which does not lend itself well to measurement by quantitative techniques. Loss of a majority of the software development team could have similar unpredictable repercussions. However, the loss of electrical power for a short duration is more easily measurable and can be quantified into monetary amounts that can be assessed with quantitative techniques.

T2-6 Which of the following would prove the **MOST** difficult to calculate an annualized loss expectancy?

A. Building fire
B. Area flood
C. Utility outage
D. Hacker attack

D Fires, floods and utility outages all occur with enough frequency that statistics have been developed that can be applied to specific organizations. Although not impossible, a hacker attack would be the most difficult to estimate with anything other than very generalized statistics.

T2-7 In performing a risk assessment on the impact of losing frame-relay network connectivity for 18-24 hours, the impact of the incident should be calculated using the:

A. hourly billing rate charged by the carrier.
B. value of the data transmitted over the network.
C. aggregate compensation of all affected business users.
D. financial losses incurred by affected business units.

D The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

T2-8 Which of the following is the **MOST** productive deliverable of an information security risk analysis?

A. A business impact analysis (BIA) report
B. A list of action items to mitigate risk
C. An assignment of risks to process owners
D. A quantification of organizational risk

B Although all of these are important, the list of action items is what will be used to reduce or transfer the current level of risk. Other options will materially contribute to the way the actions are implemented.

T2-9 Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.
C. control risk is eliminated.
D. residual risk equals transferred risk.

A Since residual risk is the risk that remains after putting into place an effective risk management program(me), acceptable risk will be achieved when this amount is minimized. Transferred risk is risk that has been assumed by a third party. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk to zero.

T2-10 For which of the following threats would the likelihood of occurrence generally be driven **MOST** by geography?

A. Power failure
B. Chemical spill
C. Explosion
D. Flooding

D Floods are naturally occurring disasters that have been tracked statistically over many years and average rates of occurrence are available for specific localities. Power failure, chemical spills and explosions are less subject to geography.

T2-11 Ongoing tracking of remediation efforts to mitigate identified risks can be accomplished **BEST** through the use of which one of the following?

A. Tree diagrams
B. Venn diagrams
C. Heat charts
D. Bar charts

C Heat charts, sometimes referred to as stoplight charts, quickly and clearly show the current status of remediation efforts. Venn diagrams show the connection between sets, tree diagrams are useful for decision analysis, and bar charts show relative size.

T2-12 Who would be in the **BEST** position to determine the recovery point objective for business applications?

A. The business continuity coordinator
B. The IS operations manager and data owners
C. The information security manager and CIO/CTO
D. Internal audit and information security managers

B The recovery point objective is the point in time to which systems will be recovered. This would be the creation date of the tapes sent offsite that would be used to restore the system. Data owners would need to make this decision in close consultation with the IS operations manager, who could offer insights on what would be technically feasible. Any decisions not involving the data owners would not provide sufficient business insights into the impact of selecting a particular RPO.

T2-13 Which two components must be assessed to make an effective judgment of the risk to an organization?

A. Visibility and duration
B. Likelihood and impact
C. Probability and frequency
D. Financial impact and duration

B A judgment involves the assessment of two components. The probability or likelihood of the event and the financial impact or magnitude of the event would be the two components. Duration refers to the length of the event, which may or may not translate into overall financial impact. No other choice includes both key factors.

T2-14 Information security managers should ideally use risk management techniques to:

A. justify their selection of risk mitigation strategies.
B. maximize the return on investment (ROI) of limited resources
C. provide documentation for auditors and regulatory bodies.
D. quantify risk values that would otherwise be qualitative.

B Information security managers should use risk management techniques to apply limited resources as efficiently as possible in the reduction of risk. None of the other choices accomplishes that task.

T2-15 In assessing risk, it is **BEST** to:

A. provide equal coverage for all asset types.
B. use experiential data from similar organizations.
C. consider both dollar value and likelihood of loss.
D. focus primarily on recent losses with the business.

C A risk analysis should take into account both the potential size and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus just on recent losses or only losses experienced by similar firms. Geography and other factors come into play as well.

T2-16 Which of the following **BEST** describes adequate protection for an asset?

A. Value of the asset and level of protection are both high
B. Ability of the attacker and level of protection are both low
C. Level of protection is low and value of the asset is high
D. Loss frequency is high and level of protection is low

A When the value of the asset is high and the protection is also high, then all that could be done to protect the asset have been done. When the level of protection is high, this reduces the probability of a successful attack. Just because the ability of the attacker is low, this does not justify a low level of protection, as some hackers with very little knowledge are able to use freely available software that requires very little technical knowledge to be effective. Any choice that describes a low level of protection is generally not going to be adequate.

T2-17 When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, the information security manager should **FIRST** notify:

A. the corporate audit committee.
B. customers who may be impacted.
C. data owners who may be impacted.
D. regulatory agencies overseeing privacy.

C The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate with the CIRT to develop a plan for corrective action. Other parties will be notified later as required by corporate policy and regulatory requirements.

T2-18 Which of the following **BEST** describes the scope of the information security manager's responsibilities for risk analysis?

A. Critical financial systems
B. Key systems and infrastructure
C. Organizational systems and processes
D. Any systems subject to regulatory compliance

C Risk analysis should include all organizational activities. It should not be limited to just certain systems or infrastructure components.

T2-19 Data owners are **PRIMARILY** responsible for creating risk mitigation strategies to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

B Data owners are responsible for approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

T2-20 Which of the following is the **MAIN** characteristic of a facilitated risk analysis process over a traditional approach?

A. It is faster and less expensive.
B. It is in the form of a peer review.
C. Risk frequencies are not considered.
D. Outside risk consultants are utilized.

A A facilitated risk assessment uses internal process owners to identify risks, their frequencies and magnitudes. As a result, it can usually be performed more quickly, without necessarily requiring outside assistance.

T2-21 Which of the following should be omitted in determining the replacement cost of a database server?

A. Installation cost
B. Insurance cost
C. Software cost
D. Memory cost

B Installation, software and memory all go into the calculation of the cost of replacing a database server. The cost of insurance would not be added as a component of replacement cost.

T3 INFORMATION SECURITY PROGRAM(ME) MANAGEMENT

T3-1 Which of the following is the **MOST** important ingredient for a successful information security program?

A. Adequate training on emerging security technologies
B. Open communication with key process owners
C. Flexible policies, standards and procedures
D. Executive management commitment and support

D Sufficient executive management support is the most important factor for the success of an information security program. Open communication, adequate training, and good policies and procedures, while important, are not as key as support from top management, because they will not ensure success if senior management support is not present.

T3-2 Which of the following is the **MOST** effective solution for preventing individuals outside the organization from modifying sensitive information on a corporate database?

A. Screened subnets
B. System access logs
C. Role-based access controls
D. Periodic entitlement reviews

A Screened subnets are DMZs and are oriented toward preventing attacks on the internal network by external users. System access logs may detect but will not prevent attacks. Role-based access controls would help ensure that users only had access to files and systems appropriate for their job role. Entitlement reviews are useful for verifying that users have proper access but would do little to prevent an external attack.

T3-3 For traveling users, which of the following is generally utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

A. An intrusion detection system
B. IP address packet filtering
C. Two-factor authentication
D. An embedded digital signature

C Two-factor authentication provides an additional security mechanism over and above that provided by passwords alone. This is frequently used by mobile users needing to establish connectivity to a corporate network. IP address packet filtering would protect against spoofing an internal address but would not provide strong authentication. An intrusion detection system can be used to detect an external attack but would not help in authenticating a user attempting to connect. Digital signatures ensure that transmitted information can be attributed to the named sender.

T3-4 What is an appropriate frequency for updating O/S patches on production servers?

A. During scheduled rollouts of new applications
B. On the last business day of each calendar month
C. Concurrently with quarterly hardware maintenance
D. Whenever important security patches are released

D Patches should be applied whenever important security updates are released. They should not be delayed to coincide with other scheduled rollouts or maintenance. Due to the possibility of creating a system outage, they should not be deployed during critical periods of application activity such as month-end or quarter-end closing.

T3-5 Which of the following devices should be placed within a DMZ?

A. Proxy server
B. Application server
C. Departmental server
D. Data warehouse server

B An application server should normally be placed within a DMZ to shield the internal network. Data warehouse and departmental servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. A proxy server forms the inner boundary of the DMZ but is not placed within it.

T3-6 A border router should be placed on a(n):

A. web server.
B. IDS server.
C. screened subnet.
D. domain boundary.

D A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

T3-7 An e-commerce order fulfillment web server should generally be placed on a(n):

A. internal network.
B. DMZ.
C. database server.
D. domain controller.

B An e-commerce order fulfillment web server should be placed within a DMZ to protect it and the internal network from external attack. Placing it on the internal network would expose the internal network to potential attack from the Internet. Since a database server should reside on the internal network, the same exposure would exist. Domain controllers would not normally share the same physical device as a web server.

T3-8 Secure customer use of an e-commerce application can **BEST** be accomplished through:

A. data encryption.
B. digital signatures.
C. strong passwords.
D. two-factor authentication.

A Encryption would be the preferred method for customers to access an e-commerce application. Strong passwords by themselves would not be sufficient, and two-factor authentication would be impractical. Digital signatures would not provide a secure means of access.

T3-9 What is the **BEST** defense against an SQL injection attack?

A. Regularly updated signature files
B. A properly configured firewall
C. An intrusion detection system
D. Strict edits on input fields

D SQL injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent being to fool the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field, so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written. Software is also available for testing for such weaknesses. All other choices would fail to prevent such an attack.

T3-10 Which of the following is the **MOST** important consideration when implementing an intrusion detection system?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

A If an intrusion detection system is not properly tuned, it will generate an unacceptable number of false-positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to O/S hardening, while encryption and packet filtering would not be as relevant.

T3-11 Which of the following is the **MOST** important consideration when securing customer credit card data acquired by a point-of-sale cash register?

A. Patching
B. Hardening
C. Encryption
D. Nonrepudiation

C Cardholder data should be encrypted using strong encryption techniques. Hardening and patching would be secondary in importance, while nonrepudiation would not be as relevant.

T3-12 Which of the following is the **BEST** method for removing system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to the appropriate managers.
B. Establish predetermined automatic expiration dates.
C. Require managers to e-mail security when the user leaves.
D. Ensure each individual has signed a security acknowledgement.

B Predetermined expiration dates are the most effective means of removing systems access for temporary users. Reliance on managers to promptly send in termination notices cannot always be counted on, while requiring each individual to sign a security acknowledgement will have little effect in this case.

T3-13 Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from:

A. corporate internal audit.
B. infrastructure management.
C. key business process owners.
D. corporate legal counsel

C Business process owners are in the best position to understand how new regulatory requirements may affect their systems. Legal counsel, infrastructure management and internal audit would not be in as good a position to fully understand all ramifications.

T3-14 Which of the following is the **MOST** important item to consider when evaluating products to monitor security across the enterprise?

A. Ease of installation
B. Product documentation
C. Telephone support
D. System overhead

D Monitoring products can impose a significant impact on system overhead for servers and networks. Product documentation, telephone support and ease of installation, while important, would be secondary.

T3-15 Which of the following is the **MOST** important consideration when using software to scan for security exposures within a corporate network?

A. Never use open source tools.
B. Focus only on production servers.
C. Follow a linear process for attacks.
D. Do not interrupt production processes.

D The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments as the test environment, if compromised, could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than linear.

T3-16 Which of the following ensures that modifications made to in-house developed business applications do not introduce new security exposures?

A. Stress testing
B. Patch management
C. Change management
D. Security baselines

C Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings, while stress testing ensures that there are no scalability problems.

T3-17 The advantage of virtual private network (VPN) tunneling for remote users is that it:

A. helps ensure that communications are secure.
B. increases security between multitier systems.
C. allows passwords to be changed less frequently.
D. eliminates the need for secondary authentication.

A VPN tunneling for remote users provides an encrypted link that helps ensure secure communications. It does not affect password change frequency, it does not eliminate the need for secondary authentication, and it does not affect security within the internal network.

T3-18 Which of the following is **MOST** effective for securing wireless networks as a point of entry into a corporate network?

A. Boundary router
B. Strong encryption
C. Internet-facing firewall
D. Intrusion detection system

B Strong encryption is the most effective means of protecting wireless networks. Boundary routers, IDS systems and firewalling the Internet would not be as effective.

T3-19 Which of the following is **MOST** effective in protecting against the attack technique known as phishing?

A. Firewall blocking rules
B. Up-to-date signature files
C. Security awareness training
D. Intrusion detection monitoring

C Phishing relies on social engineering techniques. Providing good security awareness training will best reduce the likelihood of such an attack being successful. Firewall rules, signature files and IDS monitoring will be largely unsuccessful at blocking this kind of attack.

T3-20 When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur?

A. The firewall should block all inbound traffic during the outage.
B. All systems should block new logins until the problem is corrected.
C. Access control should fall back to nonsynchronized mode.
D. System logs should switch to record all user activity for later analysis.

C The best mechanism is for the system to fallback to the original process of logging on individually to each system. Blocking traffic and new logins would be overly restrictive to the conduct of business, while recording all user activity would add little value.

T3-21 Which of the following is the **MOST** important risk associated with middleware in a client-server environment?

A. Server patching may be prevented.
B. System backups may be incomplete.
C. System integrity may be affected.
D. End-user sessions may be hijacked.

C The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely.

T4 INFORMATION SECURITY MANAGEMENT

T4-1 What is the **BEST** way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection system.
B. Establish minimum security baselines.
C. Implement vendor-recommended settings.
D. Perform periodic penetration testing.

D Penetration testing is the best way to assure that perimeter security is adequate. An IDS may detect an attempted attack, but it will not confirm whether the perimeter is secure. Minimum security baselines and applying vendor-recommended settings are beneficial, but they will not provide the level of assurance that is provided by penetration testing.

T4-2 Which of the following presents the greatest exposure to internal attack on a network?

A. User passwords are not automatically expired.
B. All network traffic goes through a single switch.
C. User passwords are encoded but not encrypted.
D. All users reside on a single internal subnet.

C When passwords are sent over the internal network in an encoded format, they can easily be converted to cleartext. All passwords should be encrypted to provide adequate security. Not automatically expiring user passwords does create an exposure, but not as great as having unencrypted passwords. Using a single switch or subnet does not present a significant exposure.

T4-3 Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

A. Standards
B. Guidelines
C. Security metrics
D. Security governance

A Standards are the bridge between high-level policy statements and the how-to, detailed format of procedures. Security metrics and governance would not ensure correct alignment between policies and procedures. Similarly, guidelines are not linkage documents but rather provide suggested guidance on best practices.

T4-4 Which of the following are the **MOST** important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer
B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal department

B Security steering committees provide a forum for management to express its opinion and take some ownership in the decision-making process. It is imperative that business process owners be included in this process. None of the other choices includes input by business process owners.

T4-5 Data owners are normally responsible for which of the following?

A. Applying emergency changes to application data
B. Administering security over database records
C. Migrating application code changes to production
D. Determining the level of application security required

D Data owners approve access to data and determine the degree of protection that should be applied (data classification). Administering database security, making emergency changes to data and migrating code to production are infrastructure tasks performed by custodians of the data.

T4-6 Which of the following is the **MOST** appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

A. System designer
B. User acceptance tester
C. Operations manager
D. System data owner

B User acceptance testers would be in the best position to note whether new exposures are introduced during the change management process. The system designer, data owner and operations manager would not be as closely involved in testing code changes.

T4-7 What is the **BEST** way to ensure that users comply with organizational security requirements for password complexity?

A. Explicitly refer to password construction requirements in the security standards.
B. Require each user to acknowledge in writing that they have read and agree to security policies.
C. Create strict penalties in the security policies for user noncompliance.
D. Implement system-enforced password requirements combined with online coaching tools.

D Automated controls are generally more effective in preventing improper actions. Policies and standards provide some deterrence, but are not as effective as automated controls.

T4-8 Which of the following represents the **MOST** significant exposure of temporary employees taking large amounts of corporate data when they complete their assignment?

A. Modems
B. USB drives
C. Printouts
D. Wireless

B USB drives can store tremendous amounts of information, which can be copied to the drive in a manner of seconds. Modems and wireless do present exposures, but not as significant with respect to the departure of temporary employees. As for printouts, these can be very bulky and would be much more noticeable than a small USB drive.

T4-9 Which of the following is the **BEST** method for deploying O/S patches to production application servers?

A. Batch all patches into annual server updates.
B. Initially load the patches on a test machine.
C. Set up servers to automatically download patches.
D. Automatically push all patches to the servers.

B Some patches can conflict with application code. For this reason, it is very important to first test all patches in a test environment to ensure that there are no conflicts with existing application systems. For this reason, C and D are incorrect as they advocate automatic updating. As for annual server updates, this would not be frequent enough to ensure adequate protection.

T4-10 Which of the following would generally be indicative of a poor metric for evaluating information security?

A. Virus signature file updates are applied to all servers every day.
B. Information security vulnerabilities are eliminated within 30 days of detection.
C. Critical patches are applied to production servers within 24 hours of their release.
D. Security incidents are formally documented within five business days of resolution.

B Due to the nature of vulnerabilities, it is not possible to completely eliminate vulnerabilities in 30 days, or even in 30 weeks. Some vulnerabilities by their nature cannot be eliminated. The timely updating of virus signature files and critical patches are good metrics, as is the timely documentation of security incidents.

T4-11 The **PRIMARY** reason for using metrics to evaluate information security is to:

A. resolve all security weaknesses.
B. justify budgetary expenditures.
C. demonstrate steady improvement.
D. raise awareness on security issues.

C The purpose of a metric is to facilitate and track continuous improvement. It will not permit the resolution of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

T4-12 What is the **BEST** method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodically examine firewall rules and router tables.
B. Review IDS logs for evidence of previous attacks.
C. Periodically perform attack and penetration tests.
D. Review server logs for evidence of hacker activity.

C Due to the complexity of firewall rules and router tables, plus the sheer size of IDS and server logs, physical review will be insufficient. The best approach for confirming the adequacy of these configuration settings is to periodically perform attack and penetration tests.

T4-13 Which of the following is **MOST** important for measuring the effectiveness of a security awareness program?

A. Questionnaires asking for participant feedback
B. A measurable evaluation of user comprehension
C. Focus group meetings to discuss improvements
D. Separate training for all new employees

B To truly judge the effectiveness of security awareness training, some means of measurable testing is necessary to confirm user comprehension. Questionnaires and focus groups may or may not provide meaningful feedback but in themselves do not provide metrics. Separate training for new employees is desirable, but it will not help in measuring effectiveness.

T4-14 Which of the following is the **MOST** important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used.
B. Set clear expectations for deliverables.
C. Monitor IDS and firewall logs closely.
D. Develop and agree upon clear rules of engagement.

D It is critical to establish a clear understanding on what is permissible during the engagement. Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used and agree on the format of the final report and any other deliverables. As for monitoring the IDS and firewall, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

T4-15 Which of the following will **BEST** prevent an employee from using a USB drive to copy files from desktop computers?

A. Restrict the available drive allocation on all PCs.
B. Disable USB ports on all desktop devices.
C. Run antispyware software on each machine.
D. Prohibit the use of USB drives on all devices.

A Restricting the ability of a PC to allocate new drive letters will ensure USB drives or even CD writers cannot be attached, as they would not be recognized by the operating system. Disabling USB ports on all machines would not be practical, since mice and other peripherals depend on these connections. Antispyware software would not detect the use of a USB drive. Prohibiting the use of USB drives will not deter someone who is already predisposed to committing an improper act.

T4-16 Which of the following is the **MOST** important area of focus when examining potential security exposures for deployment of a new wireless network?

A. Signal strength
B. Number of zones
C. Network bandwidth
D. Encryption strength

D Encryption strength is the main area where wireless networks tend to fall short. Signal strength, network bandwidth and the number of zones are all secondary issues.

T4-17 Good information security standards should:

A. define precise and unambiguous allowable limits.
B. describe the process for communicating violations.
C. address high-level objectives of the organization.
D. be updated frequently, as new software is released.

A A security standard should be very clear in what is allowable. Generally, it should not change that frequently. The process for communicating violations would be addressed by a security procedure, not a standard. High-level objectives of an organization would normally be addressed in a security policy.

T4-18 Good information security procedures should:

A. define the allowable limits of behavior.
B. communicate the importance of security governance.
C. describe security baselines for each platform.
D. be updated frequently as new software is released.

D Security procedures often have to change frequently to keep up with changes in software. Since a procedure is a how-to document, it must keep up to date with changes in software, which can occur frequently. A security standard, such as platform baselines, define behavioral limits, not the how-to process. Generally it should not change that frequently. High-level objectives of an organization such as security governance would normally be addressed in a security policy.

T4-19 What is the **MAIN** drawback of e-mailing password-protected zip files across the Internet?

A. They all use weak encryption.
B. They are decrypted by the firewall.
C. They may be quarantined by mail filters.
D. They may be corrupted by the sending mail server.

C Often, mail filters will quarantine zip files that are password-protected, since the filter (or the firewall) is unable to determine if the file contains malicious code. Many zip file products are capable of using strong encryption. Such files are not normally corrupted by the sending mail server.

T4-20 A major trading partner who has access to the internal network of an organization is either unwilling or unable to remediate serious information security exposures within its own environment. What is the **BEST** action for the information security manager to recommend?

A. Ask the trading partner to sign an agreement assuming all liability for a breach.
B. Remove all trading partner access to the internal network until the situation improves.
C. Set up firewall rules to tightly restrict network traffic to and from the trading partner.
D. Send periodic reminders to the trading partner advising them of their noncompliance.

C It is incumbent on the information security manager to see to the protection of his/her organization's network, but do so in a manner that will not adversely affect the conduct of business. Agreements and reminders will not protect the integrity of the network.

T4-21 When it is suspected that symmetric encryption keys have been compromised, which of the following is the **MOST** appropriate method for ensuring that new encryption keys are securely delivered to the authorized trading partners?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

C Out-of-band channels are useful when it is necessary for confidentiality to communicate a message through a nonroutine channel when the primary channel is known to be compromised. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting an IP address to a username. Delivery path tracing will show the route taken but not confirm the identity of the sender.

T4-22 What is the **MOST** effective method for ensuring that users do not share the same logon ID?

A. Prohibit ID sharing in the security standards
B. Automated analysis of logon ID's to detect duplicates
C. Address ID sharing in security awareness training
D. Review system logs for user login and logoff times

B Automatic analysis of logon IDs against users will detect if the same ID has been issued to more than one user enabling one to be deleted and an individual ID allocated. Prohibitions and awareness training will be less effective, as will reviewing system logs.

T4-23 Which of the following is the **MOST** immediate consequence of failing to tune a newly installed intrusion detection system with the threshold set to a low value?

A. The number of false-positives will increase.
B. The number of false-negatives will increase.
C. Active probing will be missed.
D. Attack profiles will be ignored.

A Failure to tune an IDS will result in many false-positives, especially when the threshold is set to a low value. The other options are less likely given the fact that the threshold for sounding an alarm is set to a low value.

T4-24 What is the **MOST** appropriate change management procedure for the handling of emergency program changes?

A. Formal documentation need not be completed since the change is the result of an emergency situation.
B. Review and approval by management should be obtained and documented prior to making the change.
C. All documentation should be completed, with review and approval occurring as soon as possible afterward.
D. All program changes should go through exactly the same change management process.

C Even in the case of an emergency change, all documentation should be completed. The difference lies in the timing of certain events. With an emergency change, it is permissible to obtain certain approvals and other documentation on the morning after—once the emergency has been satisfactorily resolved.

T5 RESPONSE MANAGEMENT

T5-1 When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the **MOST** important concern?

A. Ensuring accessibility should a disaster occur
B. Versioning control as plans are modified
C. Storing broken hyperlinks to resources elsewhere
D. Tracking changes in personnel and plan assets

A If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the Intranet or other systems that are not longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern but less serious than plan accessibility.

T5-2 Which of the following should be mandatory for any disaster recovery test?

A. Only materials taken from off-site storage or pre-deployed at the hot site are used.
B. Participants are not informed in advance when the test is to be held.
C. Hot site personnel are not informed in advance when the test is to be held.
D. Key systems are restored to identical O/S releases and hardware configurations.

A To ensure that a disaster recovery test is successful, it is most important to ensure that only materials taken from offsite storage or already at the hot site are used in the test. Otherwise, a true test was not conducted since such materials from the destroyed facility might not be available following a disaster. Whether or not a test was unannounced does not necessarily make it a more successful test. It would be almost impossible to not inform hot site personnel, as they schedule tests many months in advance. The use of identical O/S versions and hardware is not always possible at a hot site.

T5-3 Which of the following is included in a business impact analysis (BIA)?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of losing different systems
C. Location and cost of commercial recovery facilities
D. Estimated annualized loss expectancy from key risks

B A BIA contains the incremental daily cost of losing different systems. It does not address the cost of rebuilding, cost of hot site alternatives, or ALE estimates.

T5-4 Which of the following is the **BEST** way for the information security manager to verify that all critical production servers are utilizing up-to-date virus signature files?

A. Check the software management console to verify the date that signature files were last pushed out to the servers.
B. Copy a recently identified benign virus to a sample of servers to see if it is automatically quarantined.
C. Check the vendor's web site for the most recent signature file and compare this to the management console.
D. Check the settings on a sample of servers to verify that the signature files are current.

D The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that it was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

T5-5 Which of the following actions should be taken when an information security manager discovers that a hacker is footprinting the network perimeter?

A. Reboot the border router connected to the firewall.
B. Check IDS logs and monitor for any active attacks.
C. Update IDS software to the latest available version.
D. Enable server trace logging on the DMZ segment.

B Information security should check the IDS logs and continue to monitor the situation. It would be inappropriate to take any action beyond that. In fact, updating the IDS could create a temporary exposure until the new version can be properly tuned. Rebooting the router and enabling server trace routing would not be warranted.

T5-6 Which of the following is the **MOST** important criteria for the selection of virus protection software?

A. Product market share and annualized cost
B. Ability to interface with IDS software
C. Automatic e-mails whenever a new virus is identified
D. Ease of maintenance and frequency of updates

D For the software to be effective, it must be easy to maintain and keep current. Market share and annualized cost, links to the IDS and automatic e-mails are all secondary in nature.

T5-7 What is the **MOST** serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m.?

A. Most new viruses signatures are identified at weekends.
B. Technical personnel will not be available to support the operation.
C. Systems will be vulnerable to viruses released during the intervening week.
D. The success or failure of the operation will not be known until the following Monday.

C Updating virus signature files on a weekly basis carries the risk that the systems will be vulnerable to viruses released during the week; far more frequent updating is essential. All other issues are secondary to this, very serious exposure.

T5-8 From what source should the time and cost estimates used in a business impact analysis be derived?

A. External consultants
B. Information security
C. Business process owners
D. Industry-derived averages

C Business process owners are in the best position to understand the true impact on the business that a system outage would create. External consultants, industry averages and even information security will not be able to provide that level of detailed knowledge.

T5-9 Which of the following is **MOST** closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy
C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

D Technical recovery plans, network redundancy and equipment needs are all associated more with infrastructure disaster recovery. Only RTOs directly relate to business continuity.

T5-10 Which of the following applications would generally generate the shortest recovery time objective (RTO)?

A. Contractor payroll
B. Change management
C. E-commerce web site
D. Fixed-asset system

C In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours if not minutes. Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

T5-11 A computer incident response team (CIRT) manual should generally contain which of the following documents?

A. Risk assessment
B. Severity criteria
C. Employee phone directory
D. Table of all backup files

B Quickly ranking the severity criteria of an incident is a key element of incident response. The other choices refer to documents that would not likely be included in a CIRT manual.

T5-12 The **PRIMARY** purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

A. weaknesses in network and server security.
B. ways to improve the incident response process.
C. potential attack vectors on the network perimeter.
D. the optimum response to internal hacker attacks

A An internal attack and penetration test is designed to identify weaknesses in network and server security. It does not focus as much on incident response or the network perimeter.

T5-13 Which of the following would represent a violation of the normal rules of evidence when a backup tape has been identified as evidence in a fraud investigation? The tape was:

A. removed in the custody of law enforcement investigators.
B. kept in the tape library pending further analysis.
C. sealed in a signed envelope and locked in a safe under dual control.
D. handed over to properly authorized independent investigators.

B Since a number of individuals would have access to the tape library, the chain of custody could not be verified because any one of several individuals could have accessed and tampered with the tape; generally, this would be against the rules of evidence. All other choices provide clear indication of who was in custody of the tape at all times.

SAMPLE EXAM

1. Secure customer use of an e-commerce application can **BEST** be accomplished through:

   A. data encryption.
   B. digital signatures.
   C. strong passwords.
   D. two-factor authentication.

2. Which of the following is the **MOST** important factor when designing an information security architecture?

   A. Technical platform interfaces
   B. Scalability of the network
   C. Development methodologies
   D. Stakeholder requirements

3. What is the **MOST** appropriate change management procedure for the handling of emergency program changes?

   A. Formal documentation need not be completed since the change is the result of an emergency situation.
   B. Review and approval by management should be obtained and documented prior to making the change.
   C. All documentation should be completed, with review and approval occurring as soon as possible afterward.
   D. All program changes should go through exactly the same change management process.

4. Which of the following groups would be in the **BEST** position to perform a risk analysis for a business?

   A. External regulatory auditors
   B. A peer group within a similar business
   C. Process owners within the organization
   D. An established management consultancy

5. What is the **MOST** effective method for ensuring that users do not share the same logon ID?

   A. Prohibit ID sharing in the security standards
   B. Automated analysis of logon ID's to detect duplicates
   C. Address ID sharing in security awareness training
   D. Review system logs for user login and logoff times

6. Which of the following would be sufficient in ensuring the proper destruction of sensitive business records?

   A. Nonremovable magnetic media should be reformatted.
   B. Personal information should be rendered unrecoverable.
   C. Spoiled forms should be recycled where practical.
   D. Backup media no longer needed should be reused for other applications.

7. In assessing risk, it is **BEST** to:

A. provide equal coverage for all asset types.
B. use experiential data from similar organizations.
C. consider both dollar value and likelihood of loss.
D. focus primarily on recent losses with the business.

8. Which of the following is **MOST** closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist
B. Periodically testing network redundancy
C. Updating the hot site equipment configuration every quarter
D. Developing recovery time objectives (RTOs) for critical functions

9. Which of the following is the **MOST** important consideration when implementing an intrusion detection system?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

10. Which of the following is **MOST** likely to be a concern when distributing information security policies electronically?

A. Broken hyperlinks within the documents
B. Version control problems
C. Failure to distribute updates
D. Content being more difficult to understand

11. Which of the following is **MOST** effective in protecting against the attack technique known as phishing?

A. Firewall blocking rules
B. Up-to-date signature files
C. Security awareness training
D. Intrusion detection monitoring

12. A major trading partner who has access to the internal network of an organization is either unwilling or unable to remediate serious information security exposures within its own environment. What is the **BEST** action for the information security manager to recommend?

A. Ask the trading partner to sign an agreement assuming all liability for a breach.
B. Remove all trading partner access to the internal network until the situation improves.
C. Set up firewall rules to tightly restrict network traffic to and from the trading partner.
D. Send periodic reminders to the trading partner advising them of their noncompliance.

13. Which of the following is the **BEST** method for removing system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to the appropriate managers.
B. Establish predetermined automatic expiration dates.
C. Require managers to e-mail security when the user leaves.
D. Ensure each individual has signed a security acknowledgement.

14. What is the **BEST** method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodically examine firewall rules and router tables.
B. Review IDS logs for evidence of previous attacks.
C. Periodically perform attack and penetration tests.
D. Review server logs for evidence of hacker activity.

15. Which of the following is the **PRIMARY** reason for performing risk management?

A. It allows the organization to eliminate all risk.
B. It is a necessary part of management's due diligence.
C. It satisfies many audit and regulatory requirements.
D. It is helpful in calculating return on investment.

16. Which of the following are the **MOST** important individuals to include as members of an information security steering committee?

A. Direct reports to the chief information officer
B. IT management and key business process owners
C. Cross-section of end users and IT professionals
D. Internal audit and corporate legal department

17. Data owners are normally responsible for which of the following?

A. Applying emergency changes to application data
B. Administering security over database records
C. Migrating application code changes to production
D. Determining the level of application security required

18. Which of the following should be mandatory for any disaster recovery test?

A. Only materials taken from off-site storage or pre-deployed at the hot site are used.
B. Participants are not informed in advance when the test is to be held.
C. Hot site personnel are not informed in advance when the test is to be held.
D. Key systems are restored to identical O/S releases and hardware configurations.

19. When identifying legal and regulatory issues affecting information security, which of the following would represent the **BEST** approach to developing information security policies?

A. Create separate policy versions for each regulation.
B. Develop policies that meet all mandated requirements.
C. Incorporate policy templates provided by regulators.
D. Use commercially available policy templates.

20. Which of the following would prove the **MOST** difficult to calculate an annualized loss expectancy?

A. Building fire
B. Area flood
C. Utility outage
D. Hacker attack

21. When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur?

A. The firewall should block all inbound traffic during the outage.
B. All systems should block new logins until the problem is corrected.
C. Access control should fall back to nonsynchronized mode.
D. System logs should switch to record all user activity for later analysis.

22. Developing a successful business case for the acquisition of information security software products can **BEST** be assisted by?

A. Projecting the frequency of incidents
B. Quantifying the cost of a control failure
C. Calculating return on investment projections
D. Comparing spending against similar organizations

23. A successful risk management program should lead to:

A. optimization of risk reduction efforts vs. cost.
B. containment of losses to an annual budgeted amount.
C. identification and removal of all man-made threats.
D. elimination or transference of all organizational risks.

24. Which of the following presents the greatest exposure to internal attack on a network?

A. User passwords are not automatically expired.
B. All network traffic goes through a single switch.
C. User passwords are encoded but not encrypted.
D. All users reside on a single internal subnet.

25. Good information security procedures should:

A. define the allowable limits of behavior.
B. communicate the importance of security governance.
C. describe security baselines for each platform.
D. be updated frequently as new software is released.

26. Which of the following would represent a violation of the normal rules of evidence when a backup tape has been identified as evidence in a fraud investigation? The tape was:

A. removed in the custody of law enforcement investigators.
B. kept in the tape library pending further analysis.
C. sealed in a signed envelope and locked in a safe under dual control.
D. handed over to properly authorized independent investigators.

27. Ongoing tracking of remediation efforts to mitigate identified risks can be accomplished **BEST** through the use of which one of the following?

A. Tree diagrams
B. Venn diagrams
C. Heat charts
D. Bar charts

28. The advantage of virtual private network (VPN) tunneling for remote users is that it:

A. helps ensure that communications are secure.
B. increases security between multitier systems.
C. allows passwords to be changed less frequently.
D. eliminates the need for secondary authentication.

29. Sequencing of information security projects should be prioritized on the basis of:

A. time required to implement.
B. impact on the organization.
C. total cost to implement.
D. mix of resources required.

30. Which of the following is the **MOST** appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

A. System designer
B. User acceptance tester
C. Operations manager
D. System data owner

31. What is the **BEST** way to ensure that a corporate network is adequately secured against external attack?

A. Utilize an intrusion detection system.
B. Establish minimum security baselines.
C. Implement vendor-recommended settings.
D. Perform periodic penetration testing.

32. Which of the following should be omitted in determining the replacement cost of a database server?

A. Installation cost
B. Insurance cost
C. Software cost
D. Memory cost

33. Which of the following will **BEST** prevent an employee from using a USB drive to copy files from desktop computers?

A. Restrict the available drive allocation on all PCs.
B. Disable USB ports on all desktop devices.
C. Run antispyware software on each machine.
D. Prohibit the use of USB drives on all devices.

34. Which of the following is the **MOST** effective solution for preventing individuals outside the organization from modifying sensitive information on a corporate database?

A. Screened subnets
B. System access logs
C. Role-based access controls
D. Periodic entitlement reviews

35. Regulatory requirements relating to information security are **MOST** often directed at which of the following?

A. Offsite media storage
B. O/S patch levels
C. Personal information
D. Application recovery

36. Which of the following **BEST** describes the scope of the information security manager's responsibilities for risk analysis?

A. Critical financial systems
B. Key systems and infrastructure
C. Organizational systems and processes
D. Any systems subject to regulatory compliance

37. Which of the following is the **BEST** method for deploying O/S patches to production application servers?

A. Batch all patches into annual server updates.
B. Initially load the patches on a test machine.
C. Set up servers to automatically download patches.
D. Automatically push all patches to the servers.

38. For traveling users, which of the following is generally utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

A. An intrusion detection system
B. IP address packet filtering
C. Two-factor authentication
D. An embedded digital signature

39. Which of the following is the **MOST** important area of focus when examining potential security exposures for deployment of a new wireless network?

A. Signal strength
B. Number of zones
C. Network bandwidth
D. Encryption strength

40. The chief information security officer (CISO) should ideally have a direct reporting relationship to the:

A. Head of internal audit
B. Chief executive officer (CEO)
C. Chief technology officer (CTO)
D. Legal counsel

41. For which of the following threats would the likelihood of occurrence generally be driven **MOST** by geography?

A. Power failure
B. Chemical spill
C. Explosion
D. Flooding

42. What is the **BEST** way to ensure that users comply with organizational security requirements for password complexity?

A. Explicitly refer to password construction requirements in the security standards.
B. Require each user to acknowledge in writing that they have read and agree to security policies.
C. Create strict penalties in the security policies for user noncompliance.
D. Implement system-enforced password requirements combined with online coaching tools.

43. Which of the following would be the **MOST** appropriate task for a chief information security officer (CISO) to perform?

A. Update platform-level security settings.
B. Conduct disaster recovery test exercises.
C. Approve access to critical financial systems.
D. Develop information security strategy paper.

44. A global organization is subject to regulation by multiple governmental jurisdictions, each having differing requirements. The information security manager should:

A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
B. establish baseline standards for all locations and add supplemental standards as required
C. bring all locations into conformity with a generally accepted set of industry best practices.
D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

45. What is the **MOST** serious exposure of automatically updating virus signature files on every desktop each Friday at 11:00 p.m.?

A. Most new viruses signatures are identified at weekends.
B. Technical personnel will not be available to support the operation.
C. Systems will be vulnerable to viruses released during the intervening week.
D. The success or failure of the operation will not be known until the following Monday.

46. Acceptable risk is achieved when:

A. residual risk is minimized.
B. transferred risk is minimized.
C. control risk is eliminated.
D. residual risk equals transferred risk.

47. Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from:

A. corporate internal audit.
B. infrastructure management.
C. key business process owners.
D. corporate legal counsel

48. Which of the following is the **MOST** important action to take when engaging third-party consultants to conduct an attack and penetration test?

A. Request a list of the software to be used.
B. Set clear expectations for deliverables.
C. Monitor IDS and firewall logs closely.
D. Develop and agree upon clear rules of engagement.

49. A computer incident response team (CIRT) manual should generally contain which of the following documents?

A. Risk assessment
B. Severity criteria
C. Employee phone directory
D. Table of all backup files

50. Which of the following is the **MOST** important item of information to include in an information security standard?

A. Creation date
B. Author name
C. Initial draft approval date
D. Last review date

51. When the information security manager is developing a strategic plan for information security, the time horizon for the plan should be:

A. aligned with the IT strategic plan.
B. based on the current rate of technological change.
C. three to five years for both hardware and software.
D. aligned with the global business strategy.

52. Which of the following would generally be indicative of a poor metric for evaluating information security?

A. Virus signature file updates are applied to all servers every day.
B. Information security vulnerabilities are eliminated within 30 days of detection.
C. Critical patches are applied to production servers within 24 hours of their release.
D. Security incidents are formally documented within five business days of resolution.

53. Which of the following devices should be placed within a DMZ?

A. Proxy server
B. Application server
C. Departmental server
D. Data warehouse server

54. Which of the following is included in a business impact analysis (BIA)?

A. Cost to rebuild information processing facilities
B. Incremental daily cost of losing different systems
C. Location and cost of commercial recovery facilities
D. Estimated annualized loss expectancy from key risks

55. Which of the following is the **MOST** important consideration when using software to scan for security exposures within a corporate network?

A. Never use open source tools.
B. Focus only on production servers.
C. Follow a linear process for attacks.
D. Do not interrupt production processes.

56. When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the **MOST** important concern?

A. Ensuring accessibility should a disaster occur
B. Versioning control as plans are modified
C. Storing broken hyperlinks to resources elsewhere
D. Tracking changes in personnel and plan assets

57. Which of the following represents the **MOST** significant exposure of temporary employees taking large amounts of corporate data when they complete their assignment?

A. Modems
B. USB drives
C. Printouts
D. Wireless

58. The **BEST** way for the information security manager to prepare for regulatory reviews is to:

A. assign an information security administrator to act as a regulatory liaison.
B. perform periodic self-assessments using regulatory guidelines and reports.
C. circulate previous regulatory reports to applicable process owners.
D. refer all regulatory inquiries to the legal department.

59. Which of the following is the **MOST** important risk associated with middleware in a client-server environment?

A. Server patching may be prevented.
B. System backups may be incomplete.
C. System integrity may be affected.
D. End-user sessions may be hijacked.

60. The **PRIMARY** reason for using metrics to evaluate information security is to:

A. resolve all security weaknesses.
B. justify budgetary expenditures.
C. demonstrate steady improvement.
D. raise awareness on security issues.

61. What is the **BEST** defense against an SQL injection attack?

A. Regularly updated signature files
B. A properly configured firewall
C. An intrusion detection system
D. Strict edits on input fields

62. When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, the information security manager should **FIRST** notify:

A. the corporate audit committee.
B. customers who may be impacted.
C. data owners who may be impacted.
D. regulatory agencies overseeing privacy.

63. Which of the following is the **MAIN** characteristic of a facilitated risk analysis process over a traditional approach?

A. It is faster and less expensive.
B. It is in the form of a peer review.
C. Risk frequencies are not considered.
D. Outside risk consultants are utilized.

64. Which of the following is the **MOST** important information to include in a strategic plan for information security?

A. Information security staffing requirements
B. Current state and desired future state
C. IT capital investment requirements
D. Information security mission statement

65. Which of the following is **MOST** important for measuring the effectiveness of a security awareness program?

A. Questionnaires asking for participant feedback
B. A measurable evaluation of user comprehension
C. Focus group meetings to discuss improvements
D. Separate training for all new employees

66. Senior management commitment and support for information security can **BEST** be enhanced through:

A. publishing a formal security policy signed by the CEO.
B. regular security awareness training for new employees.
C. periodic briefings to the senior management team.
D. senior management sign-off on the information security strategy.

67. Which of the following is the **MOST** important consideration when securing customer credit card data acquired by a point-of-sale cash register?

A. Patching
B. Hardening
C. Encryption
D. Nonrepudiation

68. Which of the following is the **MOST** important item to consider when evaluating products to monitor security across the enterprise?

A. Ease of installation
B. Product documentation
C. Telephone support
D. System overhead

69. Which of the following is the **BEST** way for the information security manager to verify that all critical production servers are utilizing up-to-date virus signature files?

A. Check the software management console to verify the date that signature files were last pushed out to the servers.
B. Copy a recently identified benign virus to a sample of servers to see if it is automatically quarantined.
C. Check the vendor's web site for the most recent signature file and compare this to the management console.
D. Check the settings on a sample of servers to verify that the signature files are current.

70. Which of the following ensures that modifications made to in-house developed business applications do not introduce new security exposures?

A. Stress testing
B. Patch management
C. Change management
D. Security baselines

71. The advantage of virtual private network (VPN) tunneling for remote users is that it:

A. helps ensure that communications are secure.
B. increases security between multitier systems.
C. allows passwords to be changed less frequently.
D. eliminates the need for secondary authentication.

72. Information security managers should ideally use risk management techniques to:

A. justify their selection of risk mitigation strategies.
B. maximize the return on investment (ROI) of limited resources
C. provide documentation for auditors and regulatory bodies.
D. quantify risk values that would otherwise be qualitative.

73. Which of the following is **MOST** effective for securing wireless networks as a point of entry into a corporate network?

A. Boundary router
B. Strong encryption
C. Internet-facing firewall
D. Intrusion detection system

74. Which of the following are likely to be updated **MOST** frequently?

A. Procedures for hardening database servers
B. Standards for password length and complexity
C. Policies addressing information security governance
D. Standards for document retention and destruction

75. Who should be responsible for enforcing access rights to application data?

A. Data owners
B. Business process owners
C. The information security steering committee
D. Security administrators

76. Which of the following is the **MOST** productive deliverable of an information security risk analysis?

A. A business impact analysis (BIA) report
B. A list of action items to mitigate risk
C. An assignment of risks to process owners
D. A quantification of organizational risk

77. Data owners are **PRIMARILY** responsible for creating risk mitigation strategies to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

78. Which of the following characteristics would be the **MOST** important to look for in prospective candidates for the role of chief information security officer (CISO)?

A. Knowledge of information technology platforms, networks and development methodologies
B. Ability to understand and map organizational needs to enabling security technologies
C. Knowledge of existing regulatory environment and project management techniques
D. Ability to manage a diverse group of individuals and resources across an organization

79. Which of the following actions should be taken when an information security manager discovers that a hacker is footprinting the network perimeter?

A. Reboot the border router connected to the firewall.
B. Check IDS logs and monitor for any active attacks.
C. Update IDS software to the latest available version.
D. Enable server trace logging on the DMZ segment.

80. The **PRIMARY** motivation for developing an information security strategy is to:

A. establish security metrics and performance monitoring.
B. educate business process owners regarding their duties.
C. ensure that legal and regulatory requirements are met.
D. support the business objectives of the organization.

81. Which of the following is the **MOST** important ingredient for a successful information security program?

A. Adequate training on emerging security technologies
B. Open communication with key process owners
C. Flexible policies, standards and procedures
D. Executive management commitment and support

82. The **PRIMARY** purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

A. weaknesses in network and server security.
B. ways to improve the incident response process.
C. potential attack vectors on the network perimeter.
D. the optimum response to internal hacker attacks

83. What is an appropriate frequency for updating O/S patches on production servers?

A. During scheduled rollouts of new applications
B. On the last business day of each calendar month
C. Concurrently with quarterly hardware maintenance
D. Whenever important security patches are released

84. Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

A. Standards
B. Guidelines
C. Security metrics
D. Security governance

85. Which of the following is the **MOST** important criteria for the selection of virus protection software?

A. Product market share and annualized cost
B. Ability to interface with IDS software
C. Automatic e-mails whenever a new virus is identified
D. Ease of maintenance and frequency of updates

86. Good information security standards should:

A. define precise and unambiguous allowable limits.
B. describe the process for communicating violations.
C. address high-level objectives of the organization.
D. be updated frequently, as new software is released.

87. From what source should the time and cost estimates used in a business impact analysis be derived?

A. External consultants
B. Information security
C. Business process owners
D. Industry-derived averages

88. How frequently should information security procedures for O/S patch management generally be reviewed and updated?

A. Annually
B. Whenever standards are updated
C. Monthly
D. After every patch implementation

89. Which of the following applications would generally generate the shortest recovery time objective (RTO)?

A. Contractor payroll
B. Change management
C. E-commerce web site
D. Fixed-asset system

90. A border router should be placed on a(n):

A. web server.
B. IDS server.
C. screened subnet.
D. domain boundary.

91. When it is suspected that symmetric encryption keys have been compromised, which of the following is the **MOST** appropriate method for ensuring that new encryption keys are securely delivered to the authorized trading partners?

A. Delivery path tracing
B. Reverse lookup translation
C. Out-of-band channels
D. Digital signatures

92. Which two components must be assessed to make an effective judgment of the risk to an organization?

A. Visibility and duration
B. Likelihood and impact
C. Probability and frequency
D. Financial impact and duration

93. What is the **MAIN** drawback of e-mailing password-protected zip files across the Internet?

A. They all use weak encryption.
B. They are decrypted by the firewall.
C. They may be quarantined by mail filters.
D. They may be corrupted by the sending mail server.

94. The results of an organizational risk analysis should **FIRST** be shared with:

A. external auditors.
B. stockholders.
C. senior management.
D. peer organizations.

95. Which of the following risks would **BEST** be assessed using quantitative risk assessment techniques?

A. Customer data stolen by a former employee
B. An electrical power outage lasting 18-24 hours
C. An e-commerce web site defaced by hackers
D. The loss of 75 percent of the software development team

96. Which of the following is generally within the scope of an information security governance steering committee?

A. Interviewing candidates for information security specialist positions
B. Developing content for security awareness programs
C. Prioritizing information security initiatives
D. Approving access to critical financial systems

97. In performing a risk assessment on the impact of losing frame-relay network connectivity for 18-24 hours, the impact of the incident should be calculated using the:

A. hourly billing rate charged by the carrier.
B. value of the data transmitted over the network.
C. aggregate compensation of all affected business users.
D. financial losses incurred by affected business units.

98. Which of the following is the **MOST** immediate consequence of failing to tune a newly installed intrusion detection system with the threshold set to a low value?

A. The number of false-positives will increase.
B. The number of false-negatives will increase.
C. Active probing will be missed.
D. Attack profiles will be ignored.

99. Who would be in the **BEST** position to determine the recovery point objective for business applications?

A. The business continuity coordinator
B. The IS operations manager and data owners
C. The information security manager and CIO/CTO
D. Internal audit and information security managers

100. Which of the following **BEST** describes adequate protection for an asset?

A. Value of the asset and level of protection are both high
B. Ability of the attacker and level of protection are both low
C. Level of protection is low and value of the asset is high
D. Loss frequency is high and level of protection is low

SAMPLE EXAM ANSWER AND REFERENCE KEY

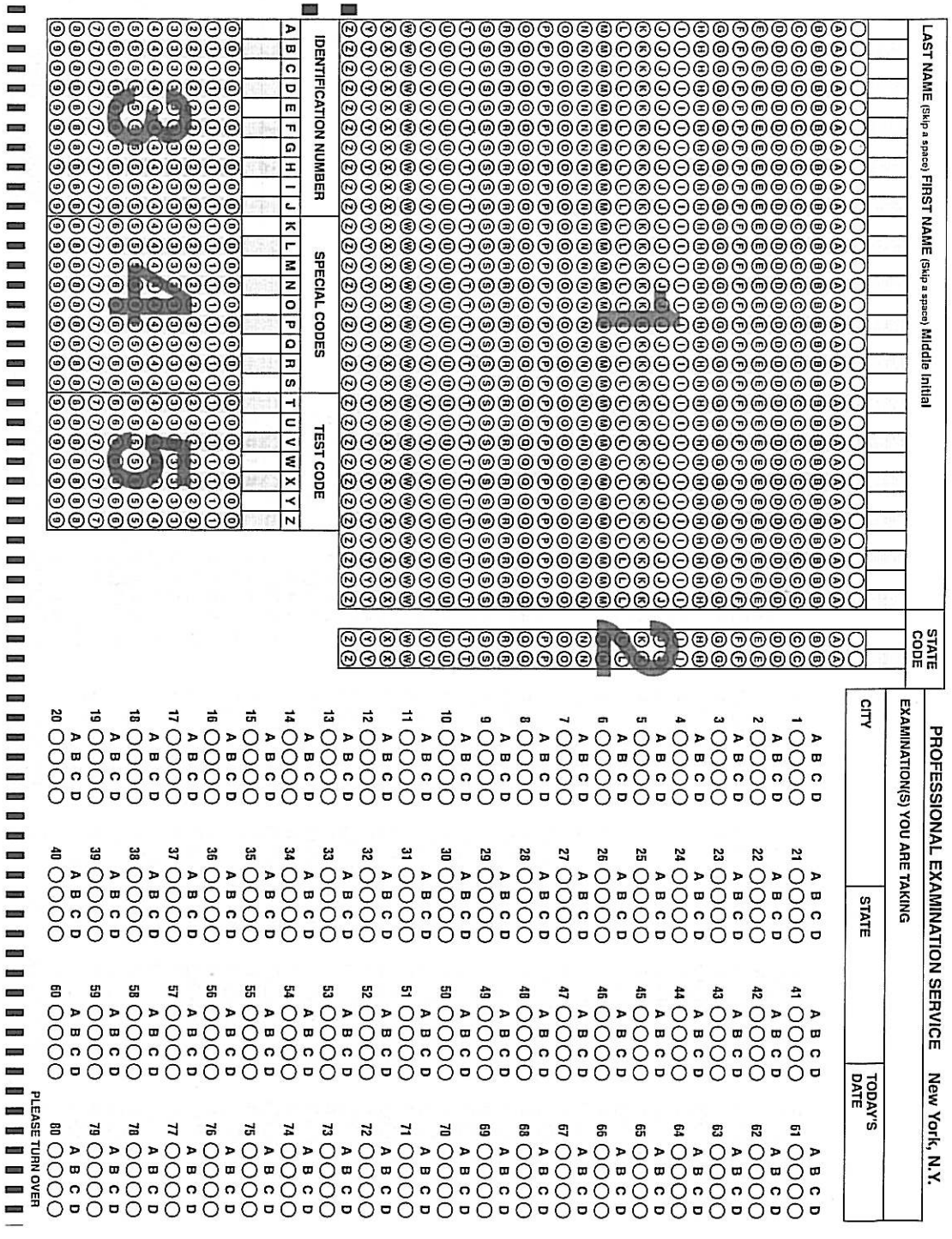
Question Number	ANSWER	REF.	Question Number	ANSWER	REF.	Question Number	ANSWER	REF.
1	A	T3-8	35	C	T1-19	69	D	T5-4
2	D	T1-5	36	C	T2-18	70	C	T3-16
3	C	T4-24	37	B	T4-9	71	A	T3-17
4	C	T2-2	38	C	T3-3	72	B	T2-14
5	B	T4-22	39	D	T4-16	73	B	T3-18
6	B	T1-12	40	B	T1-9	74	A	T1-7
7	C	T2-15	41	D	T2-10	75	D	T1-8
8	D	T5-9	42	D	T4-7	76	B	T2-8
9	A	T3-10	43	D	T1-10	77	B	T2-19
10	A	T1-17	44	B	T1-21	78	B	T1-6
11	C	T3-19	45	C	T5-7	79	B	T5-5
12	C	T4-20	46	A	T2-9	80	D	T1-1
13	B	T3-12	47	C	T3-13	81	D	T3-1
14	C	T4-12	48	D	T4-14	82	A	T5-12
15	B	T2-1	49	B	T5-11	83	D	T3-4
16	B	T4-4	50	D	T1-16	84	A	T4-3
17	D	T4-5	51	D	T1-13	85	D	T5-6
18	A	T5-2	52	B	T4-10	86	A	T4-17
19	B	T1-3	53	B	T3-5	87	C	T5-8
20	D	T2-6	54	B	T5-3	88	D	T1-18
21	C	T3-20	55	D	T3-15	89	C	T5-10
22	C	T1-11	56	A	T5-1	90	D	T3-6
23	A	T2-3	57	B	T4-8	91	C	T4-21
24	C	T4-2	58	B	T1-20	92	B	T2-13
25	D	T4-18	59	C	T3-21	93	C	T4-19
26	B	T5-13	60	C	T4-11	94	C	T2-4
27	C	T2-11	61	D	T3-9	95	B	T2-5
28	B	T3-7	62	C	T2-17	96	C	T1-4
29	B	T1-15	63	A	T2-20	97	D	T2-7
30	B	T4-6	64	B	T1-14	98	A	T4-23
31	D	T4-1	65	B	T4-13	99	B	T2-12
32	B	T2-21	66	C	T1-2	100	A	T2-16
33	A	T4-15	67	C	T3-11			
34	A	T3-2	68	D	T3-14			

Reference example: T1-1 = See section T1, question 1 for the explanation of the answer.

SAMPLE EXAM ANSWER SHEET (PRE-TEST)

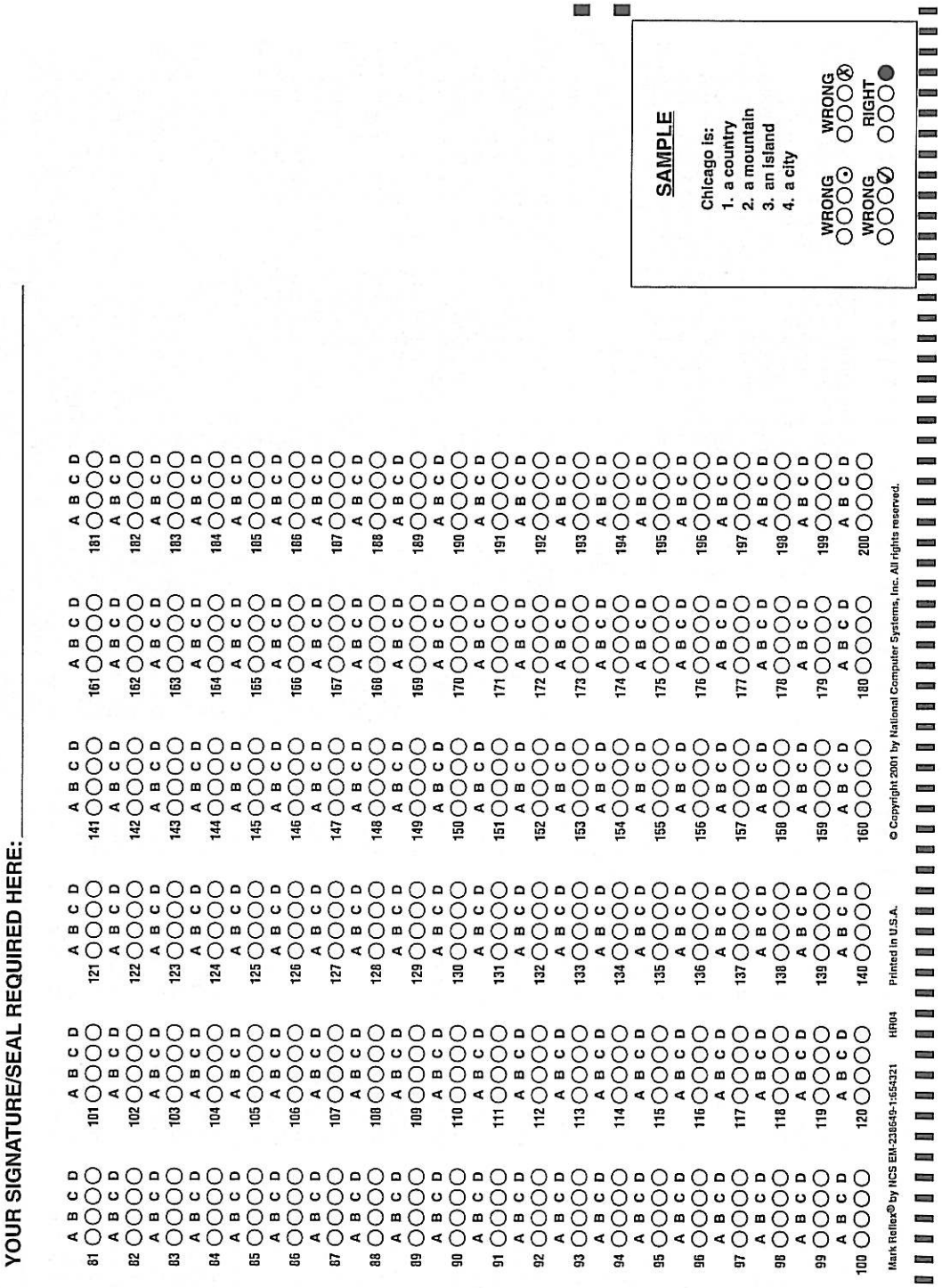
(side 1)

Please use this answer sheet if you intend to take the sample exam as a pre-test to determine strengths and weaknesses. The answer key/reference grid is on page 47



(side 2)

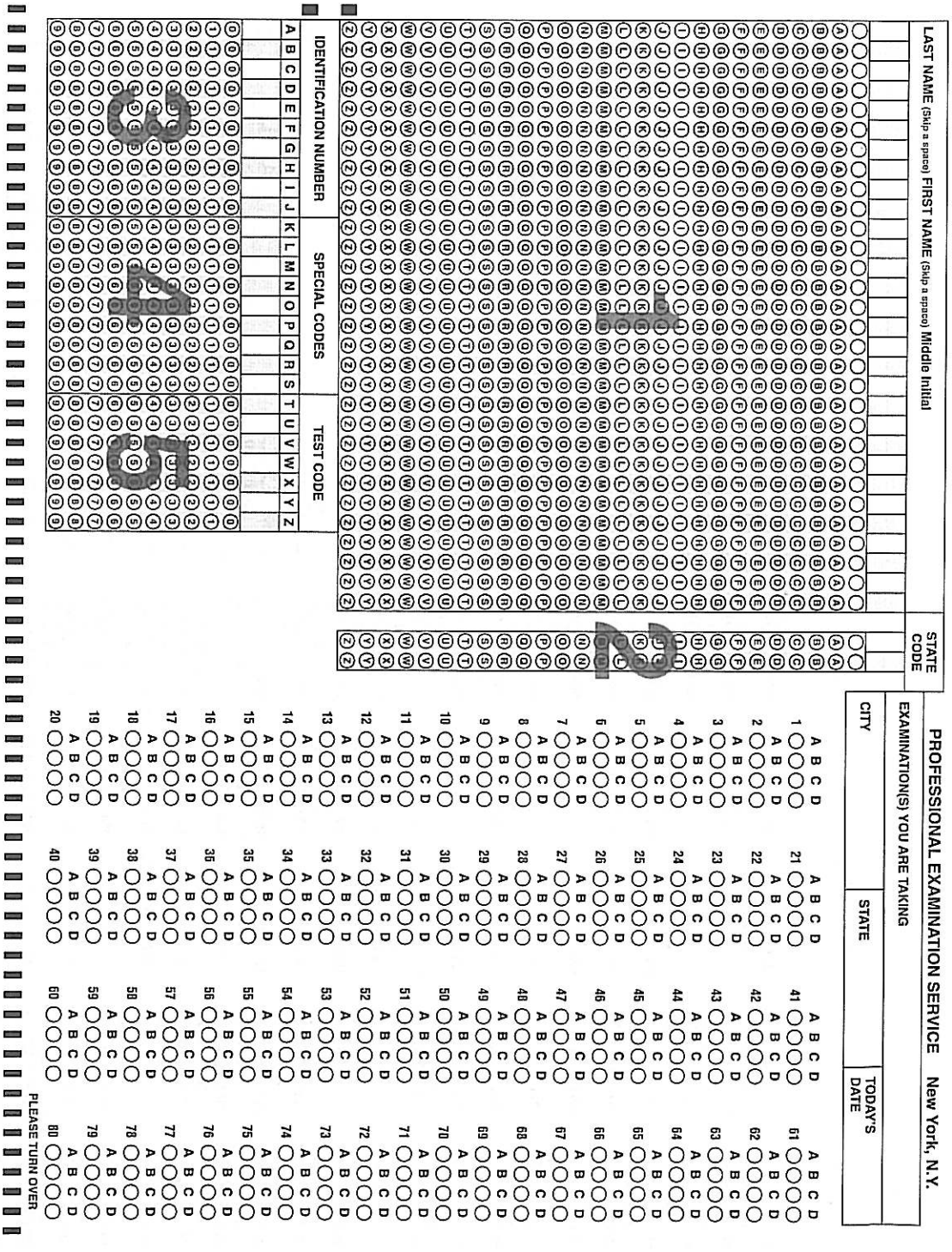
Please use this answer sheet if you intend to take the sample exam as a pre-test to determine strengths and weaknesses. The answer key/reference grid is on page 47



SAMPLE EXAM ANSWER SHEET (POST-TEST)

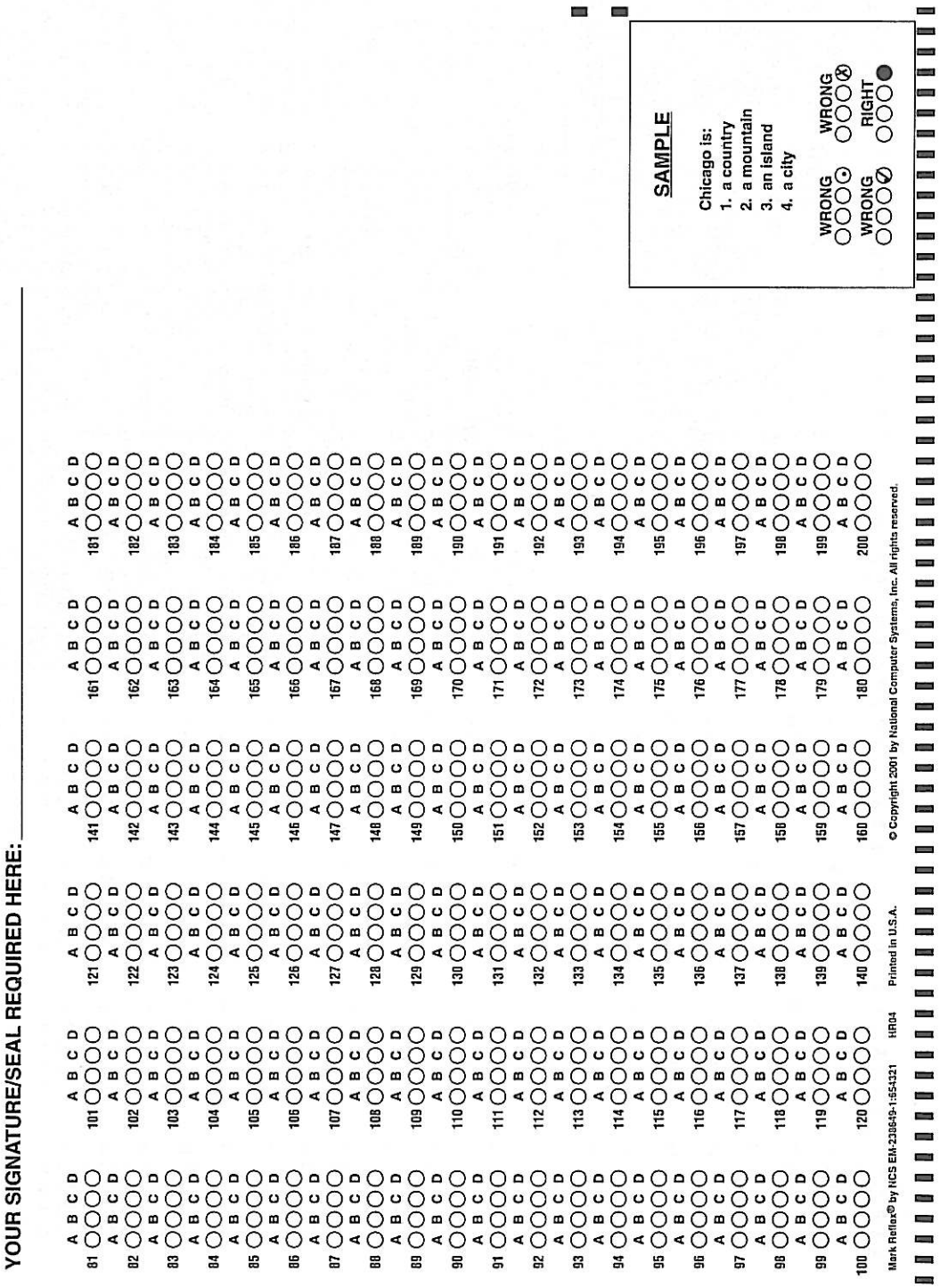
(side 1)

Please use this answer sheet if you intend to take the sample exam as a post-test to determine strengths and weaknesses. The answer key/reference grid is on page 47



(side 2)

Please use this answer sheet if you intend to take the sample exam as a post-test to determine strengths and weaknesses. The answer key/reference grid is on page 47



EVALUATION

The Information Systems Audit and Control Association continuously monitors the swift and profound professional, technological and environmental advances affecting information security managers. Recognizing these rapid advances, the CISM review materials are updated annually.

To assist the association with keeping abreast of these advances, ISACA's Board of Directors would appreciate it if you would take a moment to evaluate the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*. Such feedback is valuable to fully serve the profession and future CISM examination registrants.

Following the exam, please complete the questionnaire below and return to:

Attention: Manager—Certification Study Program and Educational Development
Mail: ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
Fax: +1.847.253.1443
E-mail: *efernandez@isaca.org*
Web site: *www.isaca.org*

1. What was your overall impression of the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*?

   ___Very helpful ___Helpful ___Not very helpful

2. Did you find the questions/answers helpful in preparing for the CISM examination?

   ___Yes ___Partially ___No

   Please explain:

   _____

   _____

   _____

3. How would you rate the format of the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement* (questions by area/sample exam)?

   ___Very helpful ___Helpful ___Not very helpful

4. What recommendations do you have for improving the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement*?

   _____

   _____

   _____

Thank You

OTHER COMMENTS/SUGGESTIONS

NOTES

Prepare for the June/December 2006 *CISM Exam*

Order Now—2006 CISM® Review Materials for Exam Preparation and Professional Development

To pass the CISM exam a candidate should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see *www.isaca.org/cismexam* for more details).

CISM Review Manual 2006

Information Systems Audit and Control Association

The *CISM Review Manual 2006* is a reference guide designed to assist individuals in preparing for the Certified Information Security Manager® (CISM®) examination and for individuals wanting to learn more about the role and responsibilities of an information security manager. The 2006 edition is significantly enhanced with changes of structure for a more comprehensive flow, updates to the content reflecting regulatory and technical changes and expanded coverage of critical areas. The manual features detailed descriptions of the tasks performed by information security managers, and the knowledge necessary to manage, design and oversee an enterprise's information security program. These task and knowledge statements were developed by the CISM Certification Board, validated by subject matter experts and serve as the blueprint for the CISM examination content and emphasis.

Information provided includes an explanation of each task and related knowledge statement, applicable information security management principles, practices and strategies. Detailed references of where to find additional guidance materials is also provided. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and review courses.

This manual has been developed and organized to assist in the study of the following job practice areas:
- Information security governance
- Risk management
- Information security program(me) management
- Information security management
- Response management

The *CISM Review Manual 2006* also provides definitions and practical examples to facilitate the learning process.

CM-6 English Edition

CISM Questions, Answers & Explanations Manual 2006

Information Systems Audit and Control Association

This manual consists of 200 multiple-choice study questions arranged in the same proportion as the CISM job analysis. Many of these items appeared in the 2004 and 2005 editions of the *CISM Review Questions, Answers & Explanations Manual*, but have been rewritten to recognize a change in practice, be more representative of the exam item format, and/or provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, and are intended to provide the CISM candidate with an understanding of the type and structure of questions and subject matter that has previously appeared on the examination.

These questions are provided in two formats.
- **Questions sorted by content area**—Questions, answers and explanations are provided (sorted) by CISM job content area. This allows the CISM candidate to study material by content area and refer to specific questions, as well as evaluate their comprehension of the topics covered within each content area.
- **Sample test**—The two hundred questions are scrambled to represent a CISM-length examination. Candidates are urged to use this sample test and the answer sheet provided to simulate an examination. Many candidates use this exam as a pretest to determine their strengths or weaknesses and/or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. All sample test questions have been cross-referenced to the questions sorted by content area, making it convenient to refer back to the explanations of the correct answers.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006 Supplement.*

CQA-6 English Edition

CISM Questions, Answers & Explanations Manual 2006 Supplement

Information Systems Audit and Control Association

This manual consists of 100 multiple-choice study questions arranged in the same proportion as the CISM job practice analysis. The questions include the answers and detailed explanations for the candidates to use in preparation for the CISM exam. Unlike some review manuals that use questions from other certification exams, these questions were prepared especially for use in studying for the CISM exam. These questions are intended to provide the CISM candidate with an understanding of the type and structure of questions that have typically appeared on the examination and are not actual test items.

This publication is ideal to use in conjunction with the *CISM Review Manual 2006* and the *CISM Review Questions, Answers & Explanations Manual 2006.*

CQA-6ES English Edition

To order the CISM review materials for the June/December 2006 CISM exam, visit our web site at *www.isaca.org/cismbooks.*

2005 CISM Review Materials are available in Japanese and Spanish.

See *www.isaca.org/nonenglishbooks.*